A Report
to the
Montana
Legislature

Information Systems Audit

Compliance and Integrity of Policy & Billing Systems

Montana State Fund

August 2023

Legislative Audit
Division

22DP-02

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives. Members of the IS audit staff hold degrees in disciplines appropriate to the audit process.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee, which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Audit Staff

Miki Cestnik
Jemma Z Hazen

Reports can be found in electronic format at:
https://leg.mt.gov/lad/audit-reports

LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
William Soller

August 2023

The Legislative Audit Committee
of the Montana State Legislature:

It is our pleasure to provide the information systems compliance audit of the Policy Center and Billing Center systems managed by the Montana State Fund.

This report provides the legislature with information about the recent system replacement and associated controls to ensure the new system operates as intended and that security, generally complies with state requirements. This report includes recommendations for improving security and compliance management at the Montana State Fund. A written response from the Montana State Fund is included at the end of the report.

We wish to express our appreciation to Montana State Fund personnel for their cooperation and assistance during the audit.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-mail lad@legmt.gov

Table of Contents

Figures and Tables

Tables

Appointed and Administrative Officials

Montana State Fund

Holly O'Dell, President/CEO (as of August 2022)

Julie Jenkinson, Vice President, Operations

Matt Coy, Vice President, Chief Information Officer

Kevin Braun, Vice President, General Counsel

Verena Maeder, Vice President, Organizational Health

State Fund Board of Directors

	Qualifications	Location	Term Expires
Richard Miltenberger, Chair	Insurance Industry Representative	Clancy	2025
Karen Fagg	Public Representative	Billings	2025
Michael Marsh	Licensed Insurance Producer	Billings	2025
John Maxness	Private Enterprise, Policyholder	Helena	2025
Nancy Butler	Private Enterprise	Helena	2027
Dexter Thiel	Private Enterprise, Policyholder	Sidney	2027
Wylie Galt	Private Enterprise, Policyholder	Martinsdale	2027

For additional information concerning the Montana State Fund, contact:

Holly O'Dell, President/CEO
855 Front Street
Helena, MT 59604
(406) 495-5015

e-mail: Holly.ODell@mt.gov

Montana Legislative Audit Division

Information Systems Compliance Audit

Compliance and Integrity of Policy & Billing Systems

Montana State Fund

A report to the Montana Legislature

Background

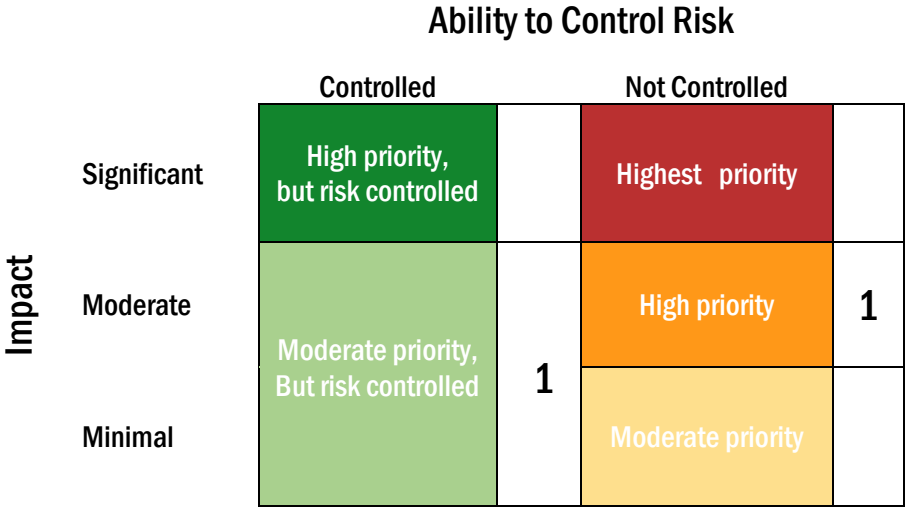
The Montana State Fund (MSF) serves the State of Montana by providing a guaranteed market for workers' compensation insurance and functions as a nonprofit private insurance carrier. "Policy and Billing Systems" refers to a suite of interconnected software systems designed to replace MSF's legacy Policy Holder System (PHS) and add enhanced, modern functionality. In concert with other established systems, the new systems constitute the infrastructure supporting MSF's core business processes related to writing, reviewing, and renewing insurance policies; providing quotes for prospective policyholders; billing and collecting insurance premiums; and processing claims.

Agency:
Montana State Fund

President/CEO:
Holly O'Dell

System Replacement Cost:
$39,880,487

Montana State Fund (MSF) successfully designed the replacement project in careful consideration of industry best practices and to increase efficiency. However, the long-term success of the systems can only be as good as the structures in place to support them. The MSF security program is not aligned with enterprise goals or state security policy and requires a role to coordinate security and compliance posture at the enterprise level.



The figure above summarizes the nature and extent of the audit findings. Findings are categorized by priority that is based on impact and whether the agency has effective controls to mitigate the risk associated with the finding. Impact is the effect a risk could have on an agency's system, security, business process, or operation. Each priority category contains the number of relevant findings in this report.

RECOMMENDATIONS:

In this report, we issued the following recommendations:
To the agency: 1
To the legislature: 0

(continued on back)

For the full report or more information, contact the Legislative Audit Division.

leg.mt.gov/lad

Room 160, State Capitol
PO Box 201705
Helena, MT 59620-1705
(406) 444-3122

The mission of the Legislative Audit Division is to increase public trust in state government by reporting timely and accurate information about agency operations, technology, and finances to the Legislature and the citizens of Montana.

To report fraud, waste, or abuse:

Online
www.Montanafraud.gov

Email
LADHotline@legmt.gov

Call
(Statewide)
(800) 222-4446 or
(Helena)
(406) 444-4446

Text
(704) 430-3930

High Priority

Recommendation #1 (page 7):

Management and operational effectiveness

Montana State Fund should establish a role that is responsible for aligning security activities with enterprise goals and is accountable for improving security and compliance posture.

Agency response: Concur

Moderate Priority, But Risk Controlled

No Recommendation

As the system moves into maintenance mode, MSF should continue to maintain the new systems with the same attention to business goals, performance metrics, and industry standards with which they designed and built it with particular attention to security infrastructure.

Chapter I – Introduction, Scope, and Objectives

Introduction

The Montana State Fund (MSF) serves the state of Montana by providing a guaranteed market for workers' compensation insurance and functions as a nonprofit, private insurance carrier. MSF's core business processes are managed by multiple software systems that support writing, reviewing, and renewing insurance policies; providing quotes for prospective policyholders; billing for and collecting insurance premiums; and processing claims. In 2015, MSF initiated a project to implement a suite of interconnected software systems to replace MSF's legacy Policy Holder System (PHS) and add enhanced, modern functionality. Based on lessons learned from industry peers, MSF first contracted with an Independent Validation & Verification (IV&V)/Organizational Change Management (OCM) vendor to assist with the framing of project objectives and to structure return on investment (ROI) criteria for evaluating the project overall. After selecting this vendor, MSF chose the software replacement for PHS and the implementation vendor to perform that replacement.

Internally the project to replace PHS was called the Policy and Billing Replacement Initiative (PBRI) and was designed to include several modular systems that interface with existing system infrastructure. The existing systems include:

- Claims Center which is the user interface that allows for the creation and processing of workers' compensations claims and leverages policyholder information from the Data Warehouse.
- The Data Warehouse, which is the database that houses the data from PHS, Claims Center and future systems of the initiative.

New systems created during PBRI include:

- Policy Center (PC), which is where policies are created, viewed and updated.
- Billing Center (BC), which bills and collects premiums from policyholders.
- Ratings Module, which is the system that Policy Center utilizes to apply the board-approved rates and tiers to new or updated policies. Policy Center should be understood to contain Ratings Module.
- Two online portals for employers and insurance policy underwriters to provide and receive quotes for prospective policies.

Policy Center and Billing Center (PC&BC) went live in November 2021. Beginning in March 2022, MSF staff transitioned each policy from the old system into the new system as the policies reached renewal. This transition process and active use of PHS concluded in March 2023. The online portals went live in September and August of 2022. The total cost of the PHS replacement and construction of the new systems as of end-of-year 2022 was $39,880,487. The final ROI for the project, based on reporting from the OCM vendor, represents a reduction in operating costs of $16,294,185 over the 10-year life cycle of the new system.

Audit Scope and Objectives

The two audit objectives were:

- Did MSF integrate industry guidelines, system interdependencies, and business process conversion when building PBRI?
- Does MSF have defined, organized, and managed processes to ensure information integrity and security?

The objectives were based on two key risks. The transition to new systems represented a significant change to business processes and information technology (IT) systems that created the potential for a loss of data integrity. Because the MSF security program had known policy gaps and was based on a framework other than the framework in state policy, there was also a concern that the MSF security program did not appropriately cover key information security controls.

Our audit focused on the implementation, design, and transition to new systems and their interoperability with existing systems. It also focused on MSF's compliance with state security policy. Included in this scope were:

- Functional requirements for PBRI, testing plans and data, and acceptance criteria.
- Data conversion and migration plans including procedures for remediation of errors.
- MSF security program policies and procedures, including user access, data classification, and control reviews.

What We Did

IT compliance audit methodologies focus on reviewing components of processes to identify how capable they are of controlling risks. Risks to the agency are identified in planning with fieldwork structured to review the processes to control or mitigate risk thoroughly. Fieldwork methodologies include:

- Identifying the individuals responsible and accountable for processes.
- Documenting a thorough understanding of control processes through interviews, observations, and document reviews.
- Reviewing any work products (reports, documents, decisions) or information sources related to reviewed processes.
- Identifying if there are metrics used for determining effectiveness.
- Assessing how the culture and behavior of staff involved in the control process influence the effectiveness.

As part of the audit, we determine how capable each control process is at meeting its intended goal and reducing risk to the agency. Table 1 (see page 3) summarizes the control areas reviewed during this audit and our overall determination. The control processes reviewed for each control area are discussed in greater detail in subsequent chapters.

Table 1
Control Areas Reviewed

Control Area	Determination
Managed Significant IT Change	3
Managed Business Process Controls	2
Legend	
Activities are organized and the process is well-defined	3
Basic activities are performed and are complete	2
Some activity occurs, yet not organized or incomplete	1
Incomplete or incompatible process	0

Source: Compiled by the Legislative Audit Division.

Criteria Used

State law outlines the responsibilities of all agencies to develop and manage security programs and conduct IT resources in an organized, deliberative, and cost-effective manner. IT governance and management practices are necessary to implement these requirements successfully.

- The State Information Security Policy (and appendices) implement Montana Code Annotated (MCA) sections that apply to information security. This policy defines the roles and responsibilities, technical controls, and IT standards adopted by the state. These standards are aligned with the National Institute of Standards and Technology (NIST) standards which map to the International Organization for Standardization (ISO) standards used in MSF's security program. Both state standards in NIST and their mapping to ISO were used as criteria during this audit engagement.
- The Common Objectives for Information and Related Technology (COBIT) framework provides guidance on common IT management and governance practices to reduce technical issues and business risks. While MSF is not required to use this standard, these practices incorporate industry best practices that support and align with NIST and State security requirements. COBIT was used to evaluate management of IT changes and business process controls for data integrity and security.
- Policies and procedures specific to MSF, including the security program, change control, data classification, and records retention provided criteria for evaluating compliance with internal requirements.
- Montana State Fund's board is required by state law to set workers' compensations rates annually based on several factors, assign those rates into tiers, and to ensure that policies be assigned to a tier at the start of each fiscal year. New business processes related to automating ratings were evaluated for data integrity.
- During the framing of PBRI, MSF created metrics for measuring project return on investment (ROI) and acceptance criteria for the software itself. These criteria provided the basis for our evaluation of the functional requirements of the project and the system.

Chapter II – Successful Management and Transition of Significant IT Change

The successful design, deployment, and use of the new systems depended on proper management of significant information technology (IT) change. We determined that MSF business and IT staff coordinated with vendor contractors during the project to design, implement, and transition to PC&BC systems while interfacing with existing systems in their IT ecosystem. The following table summarizes the significant IT change control processes reviewed in making this determination.

Table 2
Implementation Control Processes

Control Process	Determination
Management of Significant IT Change	
Establish an implementation plan	Pass
Plan business process, system and data conversion	Pass
Plan acceptance tests	Pass
Establish test environment	Pass
Perform acceptance tests	Pass
Promote to production and manage releases	Pass
Provide early production support	Pass
Perform a post-implementation review	Pass
Maintain solutions	**

Source: Compiled by the Legislative Audit Division.

** Indicates an unrated process which is discussed below.

Implementation planning: MSF business and IT staff worked with their implementation vendor to establish a body of system use cases referred to as "user stories" from the perspective of all system stakeholders. These user stories informed a narrative arc of design requirements, testing plans, acceptance criteria, and post-implementation review criteria that ensured the project was properly aligned with its goals. Adherence to this structure and well-designed development timelines enabled project staff to identify timeline milestones that were behind schedule. MSF replaced its initial implementation vendor with a peer vendor, adjusted the PBRI completion date, and ultimately finished the project at the new deadline with minimal disruptions to the initial system requirements.

Business Process and Data conversion: The user portals and Ratings Module represented functionality in the new system that didn't exist in PHS. These new features' design, implementation, and testing ensured the integrity of policy rates consistent with annual rate-setting requirements.

Deployment and early support: MSF managers designed peer training groups that leveraged subject matter experts (SMEs) to train staff and address technical and business questions during the early support period. These SMEs were the first line of support before IT staff which prevented the MSF service desk from being overwhelmed by nontechnical issues.

Maintain Solutions: Because PC&BC systems operated in tandem with the legacy system for a full year, the new system is not scheduled to move into official maintenance mode until the end of calendar year 2023. For this reason, we didn't fully evaluate these controls within the time frame of this audit engagement.

However, proper maintenance of an IT system requires many components, some of which MSF staff have completed in advance of the transition to maintenance mode. The IT operations staff have updated all support documentation, including their disaster recovery plan, which they have been able to test. MSF already has an infrastructure to support continued enhancement and support of the systems. As the system transitions to maintenance mode, a formal system maintenance plan that includes periodic reviews of operational requirements, including risk, privacy, and vulnerabilities assessments that depend on a well-managed and robust security posture, will be essential to the system's continued success.

Conclusion

MSF designed the PBRI project with appropriate controls to manage significant IT change. Continued success of the system is dependent upon formalization of a system maintenance plan and alignment of security posture.

Chapter III – Misaligned Security Posture

The Policy Center and Billing Center (PC&BC) systems' continued success depends upon well-designed and managed business process controls. These controls include alignment of control activities with business objectives, data processing integrity controls, and also security of information assets. Though MSF's key security activities are performed, we determined that the MSF security program is not aligned with business process objectives and that the MSF security program does not comply with state information security requirements.

The following table summarizes the review of the business process control activities relevant to both data processing and security of information assets.

Table 3
Security Alignment Control Processes

Control Process	Determination
Managed Business Process Controls	
Align control activities embedded in business processes with enterprise objectives	Fail
Control processing of information	Pass
Manage roles, responsibilities, access privileges and levels of authority	Fail
Manage errors and exceptions	Pass
Ensure traceability and accountability for information events	Pass
Secure information assets	Fail

Source: Compiled by the Legislative Audit Division.

Significant Findings

The significant findings in this area appear, on the surface, to be unconnected with one another. However, they are all business process controls that support and reinforce each other to ensure security aligns with business objectives, data processing integrity, access roles and responsibilities, and security of information assets.

Control alignment & compliance: One of the key activities of aligning security with business objectives is identifying compliance requirements. This ensures that the security program is designed for compliance in addition to supporting business objectives. Compliance requirements exist to establish expectations for minimum security while supporting the construction of a stable security program.

We identified three key areas where MSF's policy and procedure are misaligned with state requirements.

- **Secretary of State (SOS) records retention schedule.** MSF's operating procedure for PC&BC records is to retain them indefinitely for valid business reasons. However, internal MSF data retention guidelines are generic to all MSF information systems and do not reflect this PC&BC specific procedure or its justifications. The MSF guidelines also do not reference the SOS records retention schedule guidelines that are followed. Because internal guidelines are vague, the concern with PC&BC records retention is not that records are being improperly deleted but that they may be inefficiently retained past the point of operational requirement.

- **State data classification policy.** MSF has had data classification policies in draft since 2018, and the organization has a staff-level understanding of how data should be classified. MSF has yet to adopt its draft policy or adopt the state policy formally. This lack of formalization has caused confusion about data ownership for PC&BC systems.
- **State security policy.** The MSF security program is based on the International Organization for Standardization (ISO framework), which is commonly used in private sector and international organizations. However, ISO does not map one-to-one with the state's information security policy based on the NIST SP800-53 control framework. While MSF has a crosswalk between ISO and certain NIST publications, the crosswalk does not map to the security baseline in state policy. It is not maintained to identify gaps when changes in either standard occur. MSF has policies to address most state security requirements; however, several NIST standards were identified as gaps that MSF needs to address in its security program.

Management of roles and responsibilities: According to MSF's own security policy, security staff should review special privileges within MSF applications quarterly. A portion of this process was delegated to internal audit who should not be responsible for control actions they evaluate for effectiveness as this represents a conflict of interest for their function. Furthermore, reports checking special privileges for Policy Center were not configured properly and did not review appropriate roles within the application.

Securing information assets: The primary goal of a security program is to secure information assets. The foundation for properly doing so relies on all the above control processes being present and mature. Any gaps in these control processes result in a cascading effect. MSF performs many necessary activities to secure information assets well, and we did not identify significant risks. However, the gaps in data classification and baseline security controls reflect deficiencies in the management of the security program that need to be formalized to achieve the goals of a security program.

Impact

Each of the significant findings could be considered in terms of their specific impact to MSF operations. Though the most immediate effects appear to be noncompliance with state policy or MSF's own policies, there is a larger impact above noncompliance itself.

Those areas of the NIST framework that are missing specifically from MSF's security program have two main aspects:

- **Data classification.** When data is not classified it cannot be properly labeled and, therefore, not properly restricted from users based on the principle of least privileges. Though user access to PC&BC systems is not a specific concern based on how it has been built, the larger management of that access is unstable without proper data classification.
- **Measures of performance/plans of action and milestones.** The MSF security program does not contain specific controls for the development of a plan of action and milestones for security systems or measures of performance for security in the organization. Therefore, MSF has not developed a process for reporting on the overall effectiveness of the security function and cannot ensure updates to the security program will occur or be prioritized along with daily security activities. Without this higher-level set of controls, activities performed by security staff cannot be coordinated and aligned with business objectives.

By not complying with these aspects of the state's security framework, MSF ensures that security activities cannot be monitored for control instability and erosion, and the security program cannot be assessed for continual improvement. For example, our review uncovered several security policies that had been in draft for five years. These policies were not adopted into the security program because they required a data classification policy to be effective. Though MSF security staff were aware of both the need for data classification and the draft policies dependent on it, control gaps in plans of action and milestones obstructed progress in adopting the policies. There was no firm implementation date. Without continual monitoring of program effectiveness, these gaps in compliance and in the security policy itself cannot be identified as enterprise risks, undermining the effectiveness of MSF's business objectives.

Improvement Opportunity

Montana State Fund demonstrated how successful a project can be when it is properly aligned with business objectives. Though the project was a major undertaking that required the coordination of many teams, these entities all worked in concert. At the outset, MSF set clear success measures and was, therefore, able to demonstrate the value of the project as a whole. This represents a proper alignment of IT goals with enterprise goals and demonstrates MSF's commitment to following insurance industry standards. MSF can leverage the same orientation to improve its security management.

MSF would benefit from a structure that allows the organization to monitor its security program for continual improvement and coordinate activities with compliance and risk management functions. This could ensure compliance with state and internal security policies and provide MSF with a robust security function that complements their IT and corporate functions.

Currently, MSF has two IT security positions which are designed to assist with and provide guidance for the construction of the security program but not to set the enterprise-wide security posture. Though the security staff coordinates with compliance and risk management staff, there is no integrated role or management layer that acts as the responsible party for the enterprise's information security program.

MSF recognizes the value a best-in-class security program could have for the success of its industry partnerships and business operations. Based on trends in the insurance sector, MSF has a goal to provide industry partners with external assurances of their security posture and is taking steps to achieve this goal, despite there being no requirement to do so. While this would provide business value to MSF, it will also add more scrutiny to its security program, which will increase the need for a role to manage compliance with various security frameworks in addition to those of the state.

MSF has options in how this can be done. It could create a position specifically to establish this role, or the responsibilities could be assigned to a group of individuals. If a group is chosen, MSF will need to be deliberate in how they share the responsibilities across several positions or vest it in a specific team. The role will need to be responsible for managing security activities through careful alignment with enterprise-wide goals and accountable for improving the MSF security program and compliance posture. This would ensure compliance issues are addressed, and MSF would have a fully managed security program that is actively improving.

RECOMMENDATION #1

We recommend Montana State Fund establish a role within the organization that:

A. *Is responsible for aligning security activities and management with enterprise-wide goals and providing input to enterprise directions, and*

B. *Is accountable for the ongoing improvement and management of the security and compliance posture of State Fund.*

MONTANA STATE FUND

STATE FUND RESPONSE

Montana State Fund

P.O. Box 4759, Helena, MT 59604-4759
Customer Service 800-332-6102
Fraud Hotline 888-682-7463
(888-MT-CRIME)
montanastatefund.com

August 11, 2023

Mr. Angus Maciver
Director
Legislative Audit Division
State Capitol Building, Room 106
Helena, Montana 59620-1705

RECEIVED
August 11, 2023
LEGISLATIVE AUDIT DIV.

Dear Mr. Maciver:

Montana State Fund (MSF) appreciates the professionalism of the Legislative Audit Division staff in completing the insurance systems compliance and integrity audit of our policy and billing systems.

MSF concurs with Recommendation #1 – Management and operational effectiveness – MSF should establish a role that is responsible for aligning security activities with enterprise goals and is accountable for improving security and compliance posture.

Management has carefully evaluated the available opportunities and will establish a dedicated compliance role at MSF to work alongside a team of qualified individuals who will collectively take on the responsibilities outlined in the audit recommendation. This cross-functional team will be vested with the following responsibilities:

a. Align security activities and management with enterprise-wide goals. The team will meet on a regular basis to provide valuable input to agency objectives, ensuring that security considerations are an integral part of our strategic planning processes.
b. Ongoing improvement and management of the security and compliance posture. The team will collectively assume accountability for continuously improving our security program and compliance posture. Through close collaboration, the team will develop and implement necessary security measures, and ensure compliance with relevant regulations and industry standards.

The management and staff of MSF are very proud of our accomplishments and the high level of customer service we provide to Montana employers and employees. We value the Legislative Audit Division's assurance and assistance and value opportunities to improve our operations to ensure Montanans will benefit from a strong Montana State Fund many years into the future.

Sincerely,

Holly O'Dell
President/CEO